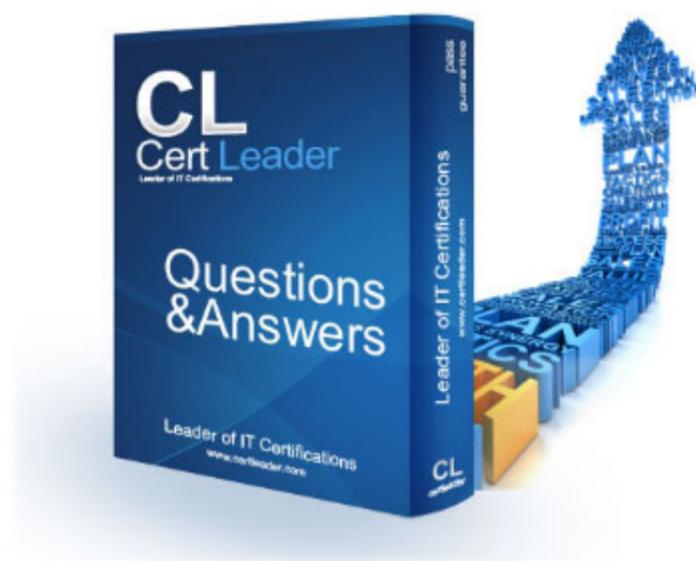


200-201 Dumps

Understanding Cisco Cybersecurity Operations Fundamentals

<https://www.certleader.com/200-201-dumps.html>



NEW QUESTION 1

Refer to the exhibit.

Top 10 Src IP Addr ordered by flows:									
Date first seen	Duration	Src IP Addr	Flows	Packets	Bytes	pps	bps	bpp	
2019-11-30 06:45:50.990	1147.332	192.168.12.234	109183	202523	13.1 M	176	96116	68	
2019-11-30 06:45:02.928	1192.834	10.10.151.203	62794	219715	25.9 M	184	182294	123	
2019-11-30 06:59:24.563	330.110	192.168.28.173	27864	47943	2.2 M	145	55769	48	

What information is depicted?

- A. IIS data
- B. NetFlow data
- C. network discovery event
- D. IPS event data

Answer: B

NEW QUESTION 2

Which type of evidence supports a theory or an assumption that results from initial evidence?

- A. probabilistic
- B. indirect
- C. best
- D. corroborative

Answer: D

NEW QUESTION 3

Refer to the exhibit.

```
Mar 6 10:35:34 user sshd[12900]: pam_unix(sshd:auth):authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1
Mar 6 10:35:36 user sshd[12900]: Failed password for invalid user not_bill from
127.0.0.1 port 38346 ssh2
```

In which Linux log file is this output found?

- A. /var/log/authorization.log
- B. /var/log/dmesg
- C. var/log/var.log
- D. /var/log/auth.log

Answer: D

NEW QUESTION 4

Drag and drop the access control models from the left onto the correct descriptions on the right.

MAC	object owner determines permissions
ABAC	OS determines permissions
RBAC	role of the subject determines permissions
DAC	attributes of the subject determines permissions

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

MAC	DAC
ABAC	MAC
RBAC	RBAC
DAC	ABAC

NEW QUESTION 5

A user received a malicious attachment but did not run it. Which category classifies the intrusion?

- A. weaponization
- B. reconnaissance
- C. installation
- D. delivery

Answer: D

NEW QUESTION 6

What is a difference between inline traffic interrogation and traffic mirroring?

- A. Inline inspection acts on the original traffic data flow
- B. Traffic mirroring passes live traffic to a tool for blocking
- C. Traffic mirroring inspects live traffic for analysis and mitigation
- D. Inline traffic copies packets for analysis and security

Answer: B

NEW QUESTION 7

Which metric is used to capture the level of access needed to launch a successful attack?

- A. privileges required
- B. user interaction
- C. attack complexity
- D. attack vector

Answer: A

NEW QUESTION 8

What should a security analyst consider when comparing inline traffic interrogation with traffic tapping to determine which approach to use in the network?

- A. Tapping interrogation replicates signals to a separate port for analyzing traffic
- B. Tapping interrogations detect and block malicious traffic
- C. Inline interrogation enables viewing a copy of traffic to ensure traffic is in compliance with security policies
- D. Inline interrogation detects malicious traffic but does not block the traffic

Answer: A

NEW QUESTION 9

What is the practice of giving employees only those permissions necessary to perform their specific role within an organization?

- A. least privilege
- B. need to know
- C. integrity validation
- D. due diligence

Answer: A

NEW QUESTION 10

What is rule-based detection when compared to statistical detection?

- A. proof of a user's identity
- B. proof of a user's action
- C. likelihood of user's action
- D. falsification of a user's identity

Answer: B

NEW QUESTION 10

Which evasion technique is a function of ransomware?

- A. extended sleep calls
- B. encryption
- C. resource exhaustion
- D. encoding

Answer: B

NEW QUESTION 13

Which regex matches only on all lowercase letters?

- A. [az]+
- B. [^az]+
- C. az+
- D. a*z+

Answer: A

NEW QUESTION 15

What are the two characteristics of the full packet captures? (Choose two.)

- A. Identifying network loops and collision domains.
- B. Troubleshooting the cause of security and performance issues.
- C. Reassembling fragmented traffic from raw data.
- D. Detecting common hardware faults and identify faulty assets.
- E. Providing a historical record of a network transaction.

Answer: CE

NEW QUESTION 19

An intruder attempted malicious activity and exchanged emails with a user and received corporate information, including email distribution lists. The intruder asked the user to engage with a link in an email. When the link launched, it infected machines and the intruder was able to access the corporate network. Which testing method did the intruder use?

- A. social engineering
- B. eavesdropping
- C. piggybacking
- D. tailgating

Answer: A

NEW QUESTION 23

The target web application server is running as the root user and is vulnerable to command injection. Which result of a successful attack is true?

- A. cross-site scripting
- B. cross-site scripting request forgery
- C. privilege escalation
- D. buffer overflow

Answer: B

NEW QUESTION 26

How does an SSL certificate impact security between the client and the server?

- A. by enabling an authenticated channel between the client and the server
- B. by creating an integrated channel between the client and the server
- C. by enabling an authorized channel between the client and the server
- D. by creating an encrypted channel between the client and the server

Answer: D

NEW QUESTION 30

Which NIST IR category stakeholder is responsible for coordinating incident response among various business units, minimizing damage, and reporting to regulatory agencies?

- A. CSIRT
- B. PSIRT
- C. public affairs
- D. management

Answer: D

NEW QUESTION 35

Which two components reduce the attack surface on an endpoint? (Choose two.)

- A. secure boot

- B. load balancing
- C. increased audit log levels
- D. restricting USB ports
- E. full packet captures at the endpoint

Answer: AD

NEW QUESTION 39

An offline audit log contains the source IP address of a session suspected to have exploited a vulnerability resulting in system compromise. Which kind of evidence is this IP address?

- A. best evidence
- B. corroborative evidence
- C. indirect evidence
- D. forensic evidence

Answer: B

NEW QUESTION 40

Which two pieces of information are collected from the IPv4 protocol header? (Choose two.)

- A. UDP port to which the traffic is destined
- B. TCP port from which the traffic was sourced
- C. source IP address of the packet
- D. destination IP address of the packet
- E. UDP port from which the traffic is sourced

Answer: CD

NEW QUESTION 45

An investigator is examining a copy of an ISO file that is stored in CDFS format. What type of evidence is this file?

- A. data from a CD copied using Mac-based system
- B. data from a CD copied using Linux system
- C. data from a DVD copied using Windows system
- D. data from a CD copied using Windows

Answer: B

NEW QUESTION 49

Which HTTP header field is used in forensics to identify the type of browser used?

- A. referrer
- B. host
- C. user-agent
- D. accept-language

Answer: C

NEW QUESTION 54

What is the difference between the ACK flag and the RST flag in the NetFlow log session?

- A. The RST flag confirms the beginning of the TCP connection, and the ACK flag responds when the data for the payload is complete
- B. The ACK flag confirms the beginning of the TCP connection, and the RST flag responds when the data for the payload is complete
- C. The RST flag confirms the receipt of the prior segment, and the ACK flag allows for the spontaneous termination of a connection
- D. The ACK flag confirms the receipt of the prior segment, and the RST flag allows for the spontaneous termination of a connection

Answer: D

NEW QUESTION 59

Which utility blocks a host portscan?

- A. HIDS
- B. sandboxing
- C. host-based firewall
- D. antimalware

Answer: C

NEW QUESTION 61

Which security principle requires more than one person is required to perform a critical task?

- A. least privilege
- B. need to know
- C. separation of duties

D. due diligence

Answer: C

NEW QUESTION 66

A SOC analyst is investigating an incident that involves a Linux system that is identifying specific sessions. Which identifier tracks an active program?

- A. application identification number
- B. active process identification number
- C. runtime identification number
- D. process identification number

Answer: D

NEW QUESTION 68

A network engineer discovers that a foreign government hacked one of the defense contractors in their home country and stole intellectual property. What is the threat agent in this situation?

- A. the intellectual property that was stolen
- B. the defense contractor who stored the intellectual property
- C. the method used to conduct the attack
- D. the foreign government that conducted the attack

Answer: D

NEW QUESTION 69

What is an example of social engineering attacks?

- A. receiving an unexpected email from an unknown person with an uncharacteristic attachment from someone in the same company
- B. receiving an email from human resources requesting a visit to their secure website to update contact information
- C. sending a verbal request to an administrator who knows how to change an account password
- D. receiving an invitation to the department's weekly WebEx meeting

Answer: B

NEW QUESTION 73

Which event is user interaction?

- A. gaining root access
- B. executing remote code
- C. reading and writing file permission
- D. opening a malicious file

Answer: D

NEW QUESTION 78

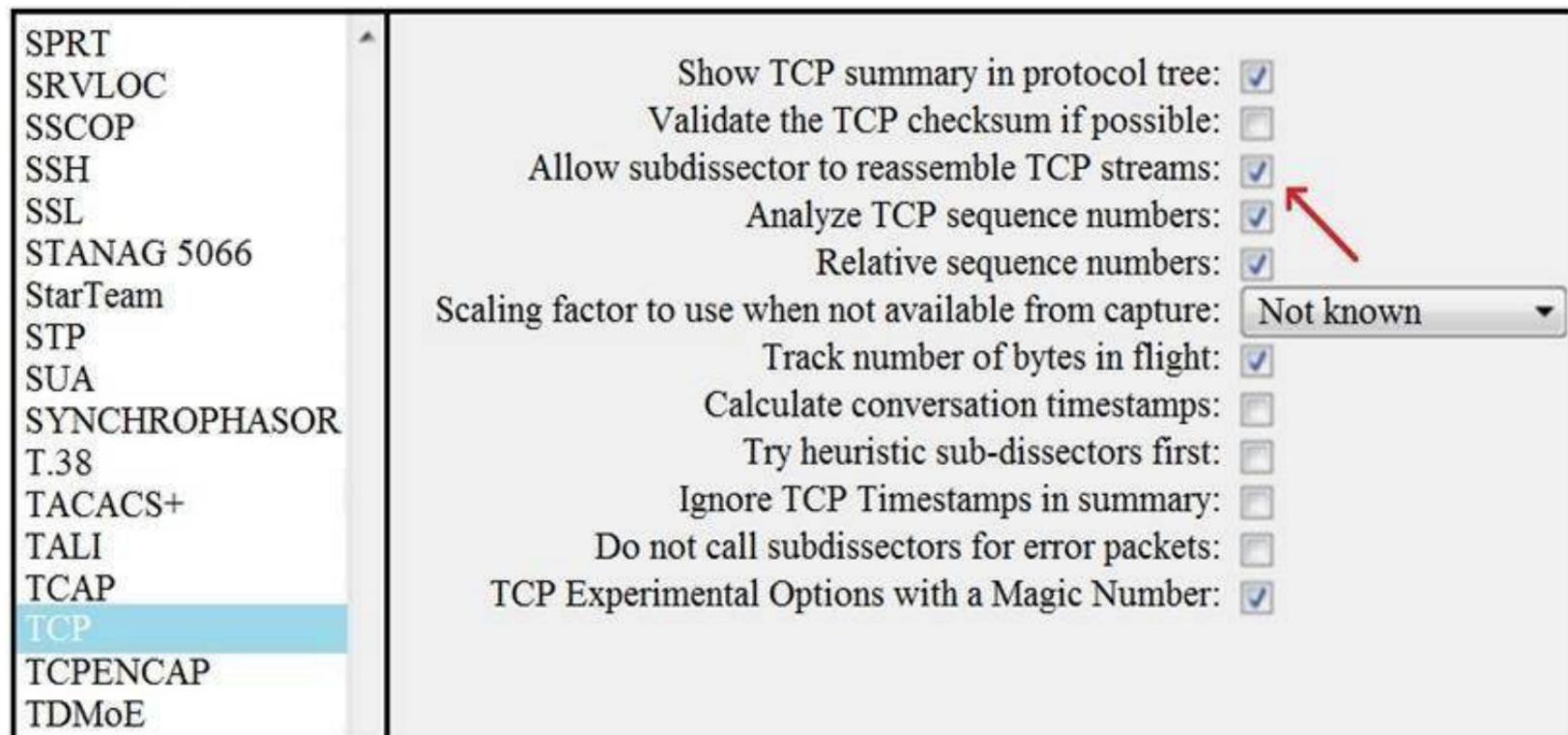
What are two social engineering techniques? (Choose two.)

- A. privilege escalation
- B. DDoS attack
- C. phishing
- D. man-in-the-middle
- E. pharming

Answer: CE

NEW QUESTION 79

Refer to the exhibit.



What is the expected result when the "Allow subdissector to reassemble TCP streams" feature is enabled?

- A. insert TCP subdissectors
- B. extract a file from a packet capture
- C. disable TCP streams
- D. unfragment TCP

Answer: D

NEW QUESTION 84

What is personally identifiable information that must be safeguarded from unauthorized access?

- A. date of birth
- B. driver's license number
- C. gender
- D. zip code

Answer: B

NEW QUESTION 87

How does an attacker observe network traffic exchanged between two users?

- A. port scanning
- B. man-in-the-middle
- C. command injection
- D. denial of service

Answer: B

NEW QUESTION 90

Which action prevents buffer overflow attacks?

- A. variable randomization
- B. using web based applications
- C. input sanitization
- D. using a Linux operating system

Answer: C

NEW QUESTION 94

Drag and drop the security concept on the left onto the example of that concept on the right.

Risk Assessment	network is compromised
Vulnerability	lack of an access list
Exploit	configuration review
Threat	leakage of confidential information

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Risk Assessment	Threat
Vulnerability	Vulnerability
Exploit	Risk Assessment
Threat	Exploit

NEW QUESTION 96

Which type of data consists of connection level, application-specific records generated from network traffic?

- A. transaction data
- B. location data
- C. statistical data
- D. alert data

Answer: A

NEW QUESTION 100

Why is encryption challenging to security monitoring?

- A. Encryption analysis is used by attackers to monitor VPN tunnels.
- B. Encryption is used by threat actors as a method of evasion and obfuscation.
- C. Encryption introduces additional processing requirements by the CPU.
- D. Encryption introduces larger packet sizes to analyze and store.

Answer: B

NEW QUESTION 104

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 200-201 Exam with Our Prep Materials Via below:

<https://www.certleader.com/200-201-dumps.html>